Dépannage de SSO dans Cisco Unified Communications Manager

Contenu

Introduction

Ce document décrit comment configurer l'authentification unique (SSO) dans Cisco Unified Communications Manager (CUCM).

Conditions préalables

Conditions requises

Cisco vous recommande de connaître les sujets suivants :

- CUCM
- Services de fédération Active Directory (ADFS)

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CUCM 11.5.1.13900-52 (11.5.1SU2)
- ADFS 2.0.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

Référez-vous à Configuration de l'authentification unique dans CUCM.

- https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-version-105/118770-configure-cucm-00.html
- https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/211302-Configure-Single-Sign-On-using-CUCM-and.html

SAML SSO Deployment Guide for Cisco Unified Communications Applications, version 11.5(1).

- https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/SAML_SSO_deployment_guide/11_5_1/CUCM_BK_S12EF288_00_saml-sso-deployment-guide--1151.html

RFC 6596 SAML.

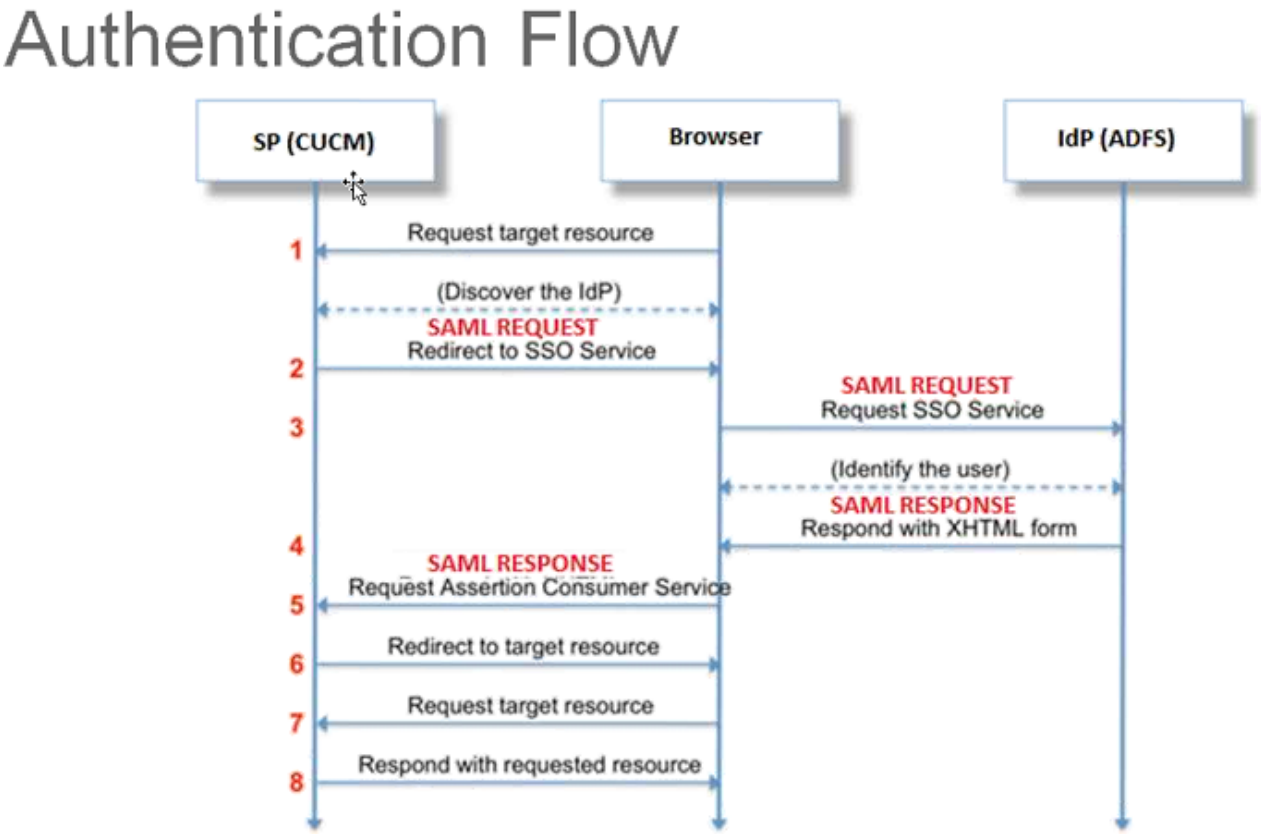
- https://tools.ietf.org/html/rfc6595

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Flux de connexion dans SSO



Décodage de la réponse SAML

Utilisation de plug-ins dans le Bloc-notes++

Installez les modules d'extension suivants :

```
Notepad++ Plugin -> MIME Tools--SAML DECODE

Notepad++ Plugin -> XML Tools -> Pretty Print(XML only – with line breaks)
```

Dans les journaux SSO, recherchez la chaîne « authentication.SAMLAuthenticator - SAML Response is :: » qui contient la réponse encodée.

Utilisez ce plugin ou le décodage SAML en ligne afin d'obtenir la réponse XML. La réponse peut être ajustée dans un format lisible avec le plug-in Pretty Print installé.

Dans la version plus récente de la réponse SAML CUCM est au format XML que vous pouvez trouver en recherchant « SPACSUtils.getResponse : get response=<samlp :

Response xmlns : samlp= “, puis imprimez avec l'utilisation du plug-in Pretty Print.

Utiliser Fiddler :

Cet utilitaire peut être utilisé pour obtenir le trafic en temps réel et le décoder. Voici le guide pour le même ; https://www.techrepublic.com/blog/software-engineer/using-fiddler-to-debug-http/.

Requête SAML :

```
ID="s24c2d07a125028bfffa7757ea85ab39462ae7751f" Version="2.0" IssueInstant="2017-07-
15T11:48:26Z" Destination="https://win-91uhcn8tt3l.emeacucm.com/adfs/ls/" ForceAuthn="false"
IsPassive="false" AssertionConsumerServiceIndex="0">
<saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">cucmsso.emeacucm.com</saml:Issuer>
<samlp:NameIDPolicy xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
SPNameQualifier="cucmsso.emeacucm.com" AllowCreate="true"/>
</samlp:AuthnRequest>
```

Réponse SAML (non chiffrée) :

```
<samlp:Response ID="_53c5877a-0fff-4420-a929-1e94ce33120a" Version="2.0" IssueInstant="2017-07-
01T16:50:59.105Z"
Destination="https://cucmsso.emeacucm.com:8443/ssosp/saml/SSO/alias/cucmsso.emeacucm.com"
Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
InResponseTo="s24c2d07a125028bfffa7757ea85ab39462ae7751f"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
<Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://win-
91uhcn8tt3l.emeacucm.com/adfs/services/trust</Issuer>
<samlp:Status>
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
</samlp:Status>
<Assertion ID="_0523022c-1e9e-473d-9914-6a93133ccfc7" IssueInstant="2017-07-01T16:50:59.104Z"
Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
```

<Issuer>http://win-91uhcn8tt3l.emeacucm.com/adfs/services/trust</Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
<ds:Reference URI="#_0523022c-1e9e-473d-9914-6a93133ccfc7">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
<ds:DigestValue>9OvwrpJVeOQsDBNghwvkLIdnf3bc7aW82qmo7Zdm/Z4=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>VbWcKUwvwiNDhUg5AkdqSzQOmP0qs5OT2VT+u1LivWx7h9U8/plyhK3kJMUuxoG/HXPQJgVQaMOwN
q/Paz7Vg2uGNFigA2AFQsKgGo9hAA4etfucIQlMmkeVg+ocvGY+8IzaNVfaUXSU5laN6zriTArxXwxCK0+thgRgQ8/46vm91
Skq2Fa5Wt5uRPJ3F4eZPOEPdtKxOmUuHi3Q2pXTw4ywZ/y89xPfSixNQEmr10hpPAdyfPsIFGdNJJwWJV4WjNmfcAqClzaG8
pB74e5EawLmwrfV3/i8QfR1DyU5yCCpxj02rgE6Wi/Ew/X/l6qSCzOZEpl7D8LwAn74KijO+Q==</ds:SignatureValue>
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>MIIC5DCCAcygAwIBAgIQZLLskb6vppxCiYP8xOahQDANBgkqhkiG9w0BAQsFADAuMSwwKgYDVQQD
EyNBREZTIFNpZ25pbmcgLSBXSU4ySzEyLnJrb3R1bGFrLmxhYjAeFw0xNTA2MjIxOTE2NDRaFw0xNjA2MjExOTE2NDRaMC4x
LDAqBgNVBAMTI0FERlMgU2lnbmluZyAtIFdJTjJLMTIucmtvdHVsYWsubGFiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApEe09jnZXEcEC7s1VJ7fMXAHPXj7jgOOcs9/Lzxrx4c68tePGItrEYnzW9vLe0Dj8OJET/Rd6LsKvuMQHfcGYqA+
XugZyHBrpc18wlhSmMfvfa0jN0Qc0lf+a3j72xfI9+hLtsqSPSnMp9qby3qSiQutP3/ZyXRN/TnzYDEmzur2MA+GP7vdeVOF
XlpENrRfaINzc8INqGRJ+1jZrm+vLFvX7YwIL6aOpmjaxcPoxDcjgEGMYO/TaoP3eXutX4FuJV5R9oAvbqD2F+73XrvP4e/w
Hi5aNrHrgiCnuBJTIxHwRGSoichdpZlvSB15v8DFaQSVAiEMPj1vP/4rMkacNQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA5
uJZI0K1Xa40H3s5MAo1SG00bnn6+sG14eGIBe7BugZMw/FTgKd3VRsmlVuUWCabO9EgyfgdI1nYZCciyFhts4W9Y4BgTH0j4
+VnEWiQg7dMqp2M5lykZWPS6vV2uD010sX5V0avyYi3Qr88vISCtniIZpl24c3TqTn/5j+H7LLRVI/ZU38Oa17wuSNPyed6/
N4BfWhhCRZAdJgijapRG+JIBeoA1vNqN7bgFQMe3wJzSlLkTIoERWYgJGBciMPS3H9nkQlP2tGvmn0uwacWPglWR/LJG3VYo
isFm/oliNUF1DONK7QYiDzIE+Ym+vzYgIDS7MT+ZQ3XwHg0Jxtr8</ds:X509Certificate>
</ds:X509Data>
</KeyInfo>
</ds:Signature>
<Subject>
<NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" NameQualifier="http:///win-
91uhcn8tt3l.emeacucm.com/com/adfs/services/trust"
SPNameQualifier="cucmsso.emeacucm.com">CHANDMIS\chandmis</NameID>
<SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<SubjectConfirmationData InResponseTo="s24c2d07a125028bfffa7757ea85ab39462ae7751f"
NotOnOrAfter="2017-07-01T16:55:59.105Z"
Recipient="https://cucmsso.emeacucm.com:8443/ssosp/saml/SSO/alias/cucmsso.emeacucm.com" />
</SubjectConfirmation>
</Subject>
<Conditions NotBefore="2017-07-01T16:50:59.102Z" NotOnOrAfter="2017-07-01T17:50:59.102Z">
<AudienceRestriction>
<Audience>ccucmsso.emeacucm.com</Audience>
</AudienceRestriction>
</Conditions>
<AttributeStatement>
<Attribute Name="uid">
<AttributeValue>chandmis</AttributeValue>
</Attribute>
</AttributeStatement>
<AuthnStatement AuthnInstant="2017-07-01T16:50:59.052Z" SessionIndex="_0523022c-1e9e-473d-9914-
6a93133ccfc7">
<AuthnContext>
<AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</AuthnCo
ntextClassRef>
</AuthnContext>
</AuthnStatement>
</Assertion>

</samlp:Réponse>

```
Version="2.0"  :- The version of SAML being used.

InResponseTo="s24c2d07a125028bfffa7757ea85ab39462ae7751f" :- The id for SAML Request to which
this reponse corresponds to

samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success :- Status Code of SAML
reponse. In this case it is Success.

<Issuer>http://win-91uhcn8tt3l.emeacucm.com/adfs/services/trust</Issuer> :- IdP FQDN

SPNameQualifier="cucmsso.emeacucm.com" :- Service Provider(CUCM) FQDN

Conditions NotBefore="2017-07-01T16:50:59.102Z" NotOnOrAfter="2017-07-01T17:50:59.102Z :- Time
range for which the session will be valid.

<AttributeValue>chandmis</AttributeValue> :- UserID entered during the login
```

Si la réponse SAML est chiffrée, vous ne pourrez pas voir l'information complète et devez désactiver le chiffrement sur Intrusion Detection & Prevention (IDP) pour voir la réponse complète. Le détail du certificat utilisé pour le chiffrement se trouve sous "ds : X509IssueSerial" de la réponse SAML.

Journaux et commandes CLI

Commandes CLI :

utils sso disable

Cette commande désactive l'authentification basée sur OpenAM SSO ou SAML SSO. Cette commande répertorie les applications Web pour lesquelles SSO est activé. Entrez **Yes** lorsque vous y êtes invité afin de désactiver SSO pour l'application spécifiée. Vous devez exécuter cette commande sur les deux noeuds dans un cluster. SSO peut également être désactivé à partir de l'interface utilisateur graphique (GUI) et sélectionnez le bouton **Désactiver**, sous SSO spécifique dans l'administration de Cisco Unity Connection.

Syntaxe de commande
utils sso disable

utils sso status

Cette commande affiche les paramètres d'état et de configuration de SAML SSO. Il permet de vérifier l'état de l'authentification unique, activée ou désactivée, sur chaque noeud individuellement.

Syntaxe de commande
utils sso status

utils sso enable

Cette commande renvoie un message texte informatif qui invite l'administrateur à activer la fonction SSO uniquement à partir de l'interface utilisateur graphique. Impossible d'activer les SSO basés sur OpenAM et SAML avec cette commande.

Syntaxe de commande
utils sso enable

utils sso recovery-url enable

Cette commande active le mode SSO de l'URL de récupération. Il vérifie également que cette URL fonctionne correctement. Vous devez exécuter cette commande sur les deux noeuds dans un cluster.

Syntaxe de commande
utils sso recovery-url enable

utils sso recovery-url disable

Cette commande désactive le mode SSO de l'URL de récupération sur ce noeud. Vous devez exécuter cette commande sur les deux noeuds dans un cluster.

Syntaxe de commande
utils sso recovery-url disable

set samltrace level <trace-level>

Cette commande active les traces et les niveaux de suivi spécifiques qui peuvent localiser toute erreur, débogage, information, avertissement ou fatale. Vous devez exécuter cette commande sur les deux noeuds dans un cluster.

Syntaxe de commande
set samltrace level <trace-level>

show samltrace level

Cette commande affiche le niveau de journal défini pour SAML SSO. Vous devez exécuter cette commande sur les deux noeuds dans un cluster.

Syntaxe de commande
show samltrace level

Suivre le moment du dépannage :

Par défaut, les journaux SSO ne sont pas définis au niveau détaillé.

Exécutez d'abord la commande **set samltrace level debug** afin de définir les niveaux de journal à déboguer, reproduire le problème et collecter ces ensembles de journaux.

Àpartir de RTMT :

Cisco Tomcat

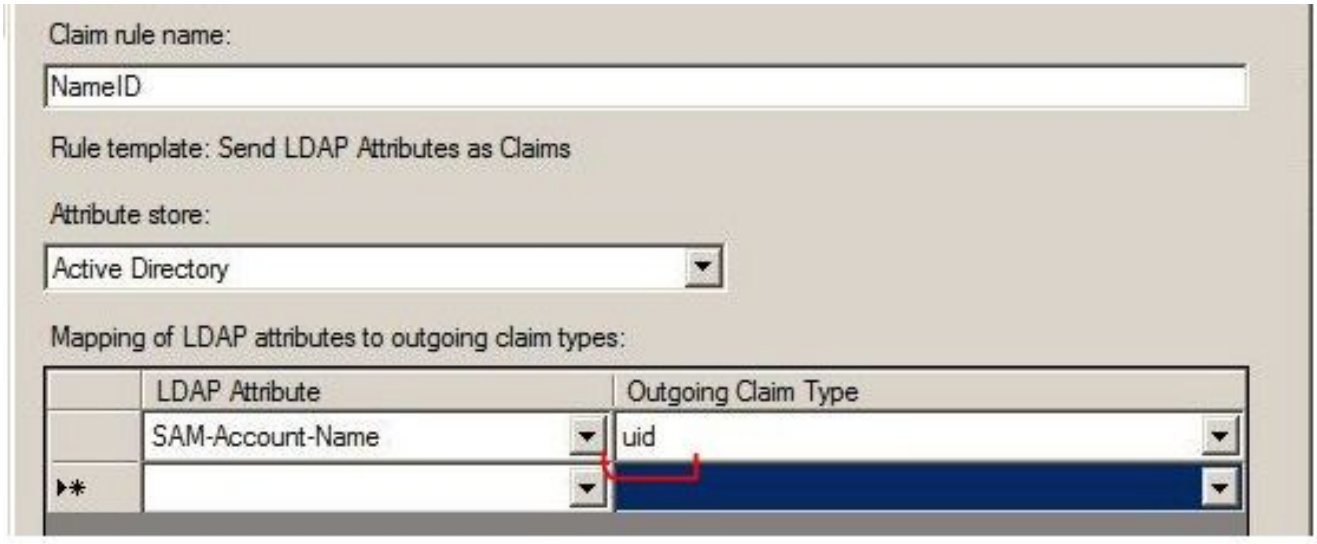
Sécurité Cisco Tomcat

SSO Cisco

Problèmes courants

Valeur incorrecte pour l'identificateur unique (UID) :

Il devrait être exactement UID et si ce n'est pas le cas, CUCM ne peut pas le comprendre.



Règle de revendication incorrecte ou stratégie NameID incorrecte :

Il est très probable qu'aucun nom d'utilisateur et mot de passe n'est demandé dans ce scénario.

Il n'y aura aucune assertion valide dans la réponse SAML et le code d'état sera le suivant :

```
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy"/>
```

Vérifiez que la règle de revendication est correctement définie du côté PCI.

Différence entre le nom et la casse Définie dans la règle de revendication :

Le FQDN CUCM dans la règle de revendication doit correspondre exactement à celui spécifié sur le serveur réel.

Vous pouvez comparer l'entrée dans le fichier xml de métadonnées de IDP à celle de CUCM en exécutant la commande **show network cluster/show network etho details** sur l'interface de ligne de commande de CUCM.

Heure incorrecte :

NTP entre CUCM et IDP a une différence supérieure aux 3 secondes autorisées dans le Guide de déploiement.

Signataire d'assertion non approuvé :

Au moment de l'échange des métadonnées entre IDP et CUCM (fournisseur de services).

Les certificats sont échangés et, en cas de révocation de certificat, les métadonnées doivent être échangées à nouveau.

Erreur de configuration DNS/Aucune configuration

DNS est la principale condition requise pour que SSO fonctionne. Exécutez **show network etho detail**, **utils diagnostic test** sur l'interface de ligne de commande afin de vérifier que DNS/Domain est configuré correctement.

Défauts connus

CSCuj66703

Le certificat de signature ADFS se renouvelle et ajoute deux certificats de signature aux réponses IDP à CUCM (SP), ce qui vous fait courir un défaut. Vous devez supprimer le certificat de signature qui n'est pas requis

CSCvf63462

Lorsque vous accédez à la page SSO SAML à partir de CCM Admin, vous êtes invité à indiquer « Les serveurs suivants ont échoué lors de la tentative d'obtention de l'état SSO », suivi du nom du noeud.

CSCvf96778

L'authentification unique CTI échoue lors de la définition du serveur CUCM en tant qu'adresse IP dans CCMAdmin//System/Sever.